Análisis de la Ingeniería Social en Instituciones de Salud

Jovanna Miranda Mollinedo
Postgrado en Informática
Universidad Mayor de San Andrés
La Paz - Bolivia
yoisa076@gmail.com

***Resumen*—Este trabajo de investigación muestra las necesidades del área de salud en materia de implementación de políticas y controles para el resguardo de la información ante ataques de Ingeniería Social. Se trata de alcanzar los objetivos establecidos, mediante nuevas prácticas e investigaciones realizadas como ser los activos que componen una institución de salud, las amenazas a la seguridad de la información, así como las medidas de seguridad disponibles para abordarlas.**

Palabras clave—ingeniería social, salud, seguridad, datos.

I. INTRODUCCIÓN

En la actualidad cualquier empresa u organización sin importar su rubro o tamaño puede ser víctima de un ataque informático. La seguridad no es un tema solo de las empresas grandes, ya que con la expansión de la tecnología los ciberdelincuentes buscan nuevos objetivos, aún más sabiendo que estas, generalmente no cuentan con adecuadas medidas de seguridad, ya que a menudo carecen de los recursos y personal necesarios para protegerse y por el gran número de activos significativos en las entidades de salud (vida del paciente, información personal confidencial y recursos financieros), la seguridad de la información es una cuestión clave para los hospitales y entidades de salud.

Sin embargo, las amenazas a las instituciones de salud no se limitan a las acciones maliciosas en términos de su causa raíz. Los errores humanos y los fallos del sistema, así como los fallos de terceros, también desempeñan un papel importante. Los riesgos que resultan de estas amenazas y de las vulnerabilidades correspondientes se mitigan normalmente mediante una combinación de medidas de seguridad organizativas y técnicas adoptadas por los hospitales inteligentes que incluyen buenas prácticas. Con respecto a las medidas organizativas, el cumplimiento de las normas, la formación y sensibilización del personal, una organización de seguridad sólida y el uso de directrices y buenas prácticas son especialmente pertinentes. Las medidas técnicas pertinentes incluyen la segmentación de la red, la gestión de activos y configuración, la monitorización de la red y la detección de intrusos. Sin embargo, los fabricantes de sistemas y dispositivos de información utilizados en los hospitales y entidades de salud también tienen que tomar ciertas medidas. Entre ellos se encuentran, por ejemplo, la integración de la seguridad en los productos desde el principio.

En la actualidad los ataques a los que son víctima las organizaciones con mayor frecuencia inician con la Ingeniería Social, para desencadenar en otros ataques como infección de malware, phishing, fraude interno o externo, entre otras [1].

Hoy en día, solo alrededor del 3% del malware intenta explotar una falla exclusivamente técnica. El otro 97% apunta a los usuarios a través de Ingeniería Social, es decir, un enfoque en el que los atacantes usan a los humanos como canales para alcanzar su objetivo. Los intentos de piratería se centran cada vez más en las vulnerabilidades humanas de un sistema de elaboración de información en lugar de fallas en el software o el hardware. Esta es una tendencia creciente [2].

La asistencia médica no solo es rápida y estresante, sino que también es una industria fuertemente regulada. Quienes trabajan en esta, necesitan hacer las cosas bien, rápido y cumplir con la legislación como HIPAA e HITECH (en los EE. UU.). Eso en sí mismo es bastante difícil, pero cuando uno combina eso con el hecho de que los actores de amenazas más comunes en esta industria son internos a la organización, puede representar una imagen bastante desafiante.

El Informe de Investigaciones de Violación de Datos del 2019 muestra que la mayoría de las víctimas de ciberataques fueron organizaciones del sector público con un 16% y en segundo lugar fueron instituciones de atención medica con un 15%, en esta se destaca que las infracciones asociadas son provenientes de actores internos. En este informe también se observa que el 52% de los ataques fue por piratería y el 33% por ingeniería social [3].

Para un hospital UW Medical en Seattle, un ataque de ingeniería social terminó con el acceso de piratas informáticos a registros médicos de 90,000 pacientes [4].

Otro estudio realizado por el Instituto Ponemon sobre el costo por violación de datos muestra que el sector salud encabeza este con un costo promedio de $ 408 por violación de datos [5].

Las normas y políticas destinadas a mantener las pantallas bloqueadas, escritorios limpios, identificar a personas que no cuentan con credenciales de identificación en áreas del negocio y aplicar controles de acceso a la infraestructura, son medidas de protección física que deben incorporarse en una organización.

En la actualidad existen muchas herramientas y técnicas que de forma relativamente fácil permiten que personas no autorizadas puedan tener acceso a la información confidencial de las organizaciones, cuando los controles no están bien implementados o no existen logran su objetivo con poco

Para referenciar este artículo (IEEE):
[N] J. Miranda, «Análisis de la Ingeniería Social en Instituciones de Salud» *Revista PGI. Investigación, Ciencia y Tecnología en Informática*, nº 7, pp. 56-61, 2020.

esfuerzo y conocimiento, causando graves perjuicios a la empresa.

La ISO 27001 se aplica a empresas de todo tipo, tamaño y sector, que manejan información sensible, pero es especialmente importante en las empresas del Sector Salud que requieren de un trato prudente de la información de los pacientes, para evitar el acceso no autorizado y la pérdida de datos (Historial clínico, notas de enfermería, datos financieros, de proveedores, etc.). Los datos e información relacionada con los pacientes deben estar bien manejados para garantizar la calidad de la asistencia sanitaria, cómo almacenar y acceder a la información de los historiales clínicos. El conocimiento de esta información por personas no deseadas puede dañar gravemente la intimidad personal y familiar, por lo que la confidencialidad de esta información es importante [6].

Es por esta razón que surge una vulnerabilidad y riesgos dentro de la seguridad de los datos que se maneja en los Centros de Salud y debido al alto grado de importancia de los archivos que maneja la institución, puede producir un significativo impacto en el aspecto clínico de los pacientes y en los servicios que presta la organización, lo que conlleva a sanciones económicas y legales, ya que la imagen y los niveles de competitividad del centro de salud pueden verse comprometidos.

II. Métodos

El método de investigación del presente trabajo es el deductivo ya que es una estrategia de razonamiento empleada para deducir conclusiones lógicas a partir de una serie de premisas o principios, comienza examinando los hechos en sí y en el proceso desarrolla una teoría coherente para representar lo que se observa, ósea el enfoque deductivo se basa en una lógica y proceso inductivo (explorar y describir y luego generar perspectivas teóricas). Este tipo de enfoque va de lo particular a lo general.

A. Diseño de la investigación.

El diseño de investigación es de corte transversal, el cual se define como el diseño de una investigación observacional, individual, que mide una o más características (variables), en un momento dado. La información de un estudio transversal se recolecta en el presente y, en ocasiones, a partir de características pasadas o de conductas o experiencias de los individuos [7].

B. Nivel de la investigación.

Exploratorio, focaliza el tópico de interés, formula problemas y delimita futuras investigaciones

Propositiva, propone en base al análisis de información un modelo apropiado.

Evaluativa, en el cual impartirá recomendaciones con base a la evaluación de los resultados.

C. Fuentes y diseño de los instrumentos de relevamiento de información

La técnica usada para el diseño e instrumentos de relevamiento de información es de tipo primaria, que permiten obtener información de primera mano a través de entrevistas, encuestas o la observación directa a ser aplicados en los sujetos de investigación.

D. Procesamiento y análisis de datos

Se usa la Estadística Descriptiva que es un conjunto de técnicas usadas para describir, representar, inferir y resumir la información del fenómeno de estudio, apoyado con programas computacionales. Iniciando con la estructuración, transcripción y análisis de datos.

III. Resultados

Existen numerosas metodologías disponibles para la realización de análisis de vulnerabilidades y amenazas una de esta son las normas ISO 27005:2018, para determinar y evaluar los tipos de Ingeniería Social en los Centros de Salud se debe tener en cuenta los siguientes aspectos:

A. Activos.

Los hospitales tienen una amplia gama de activos que son esenciales para su funcionamiento y que, por lo tanto, necesitan ser protegidos:

1. Los activos del sistema de teleasistencia como ser los equipos médicos de televigilancia y tele diagnóstico, equipo médico para la distribución de medicamentos, equipo de telesalud, como cámaras y sensores.
2. Los dispositivos médicos en red, como ser dispositivos de medición de la glucosa, bombas de insulina portátiles, marcapasos cardíacos, escáneres de tomografía computarizada.
3. Los sistemas de identificación se utilizan para rastrear y autenticar a los pacientes o al personal como ser elementos del sistema de identificación como etiquetas, brazaletes, etiquetas y tarjetas inteligentes, CCTV (videovigilancia) y escáneres biométricos.
4. Los equipos de red como ser medios de transmisión, tarjetas de interfaz de red y dispositivos de red troncal.
5. Clientes móviles, por ejemplo, ordenadores portátiles, tabletas, teléfonos inteligentes, buscapersonas, también están las aplicaciones móviles para smartphones y tablets, aplicaciones de alarma y comunicación de emergencia para dispositivos móviles.
6. Los sistemas de información clínica interconectados como los Sistemas de Información Hospitalaria (HIS), de laboratorio (LIS), de radiológica (SIF), farmacéutica (PIS), de patológica, de bancos de sangre, de archivo y comunicación de imágenes (PACS) y sistemas de investigación.
7. Los datos se consideran a menudo activos importantes desde el punto de vista de la seguridad de la información como ser: datos clínicos y administrativos del paciente, datos financieros, organizativos y otros datos hospitalarios, datos de investigación, datos de personal y datos del proveedor.
8. Los edificios e instalaciones como los sistemas de regulación de energía y clima, incluyendo sistemas inteligentes de ventilación, sensores de temperatura, y suministro de gas medicinal.

B. Análisis de amenazas

Las causas fundamentales de las amenazas a las que se enfrentan los hospitales inteligentes son las acciones maliciosas, los errores humanos, los fallos del sistema y de terceros y los fenómenos naturales.

Las acciones maliciosas son actos deliberados de una persona o de una organización como los malwares (gusanos, troyanos, rootkits, exploitkits, virus).

- El secuestro puede realizarse a nivel de red (secuestro de red/sesión - HTTP/TCP) o a nivel de dispositivo.
- La manipulación de dispositivos médicos es otra amenaza crítica.
- Los ataques de ingeniería social (por ejemplo, phishing, cebos) desempeñan un papel especial en el contexto de los hospitales inteligentes. Los ataques sociales son populares, ya que el elemento humano suele ser el eslabón más débil en la defensa de una organización.
- El robo de dispositivos y datos también es relevante en el contexto de los ataques maliciosos.
- Los ataques de denegación de servicio pueden hacer que un sistema o servicio no esté disponible.

1. Los errores humanos ocurren durante la configuración u operación de dispositivos o sistemas de información, o durante la ejecución de procesos. Los errores humanos suelen estar relacionados con procesos inadecuados o con una formación insuficiente.

- Error de configuración del sistema médico.
- Ausencia de registros de auditoría que permitan un control adecuado.
- El control de acceso no autorizado.
- Incumplimiento, especialmente en el paradigma Bring Your Own Device (BYOD).
- Los errores del médico y/o del paciente.

2. Los fallos de los sistemas son muy relevantes en el contexto sanitario, especialmente debido a la creciente complejidad y dinámica de los sistemas.

- Fallas de software.
- Firmware inadecuado.
- Los fallos de los dispositivos.
- El fallo de los componentes de la red.
- Un mantenimiento insuficiente.
- La sobrecarga puede provocar la indisponibilidad de un sistema o servicio.

3. Las fallas en la cadena de suministro están fuera del control directo de la organización afectada, ya que normalmente afectan o caen bajo la responsabilidad de un tercero.

- Proveedores de servicios en nube.
- Fabricante de dispositivos médicos.
- Proveedores de red.
- Proveedores de energía.

4. Los fenómenos naturales también pueden ser la causa de incidentes, en particular debido a sus efectos perturbadores o destructivos, en particular en las instalaciones sanitarias de los hospitales e instituciones de salud y en la infraestructura de las TIC.

- Terremotos
- Inundación
- Incendios

Los actores de las amenazas en los hospitales e instituciones de salud incluyen:

- Amenazas internas: Se trata del personal de la institución con intenciones maliciosas. Podría tratarse de médicos, enfermeras o incluso personal administrativo que tiene la intención maliciosa de dañar los sistemas de TIC. Estos pueden ser los actores potencialmente más perjudiciales.
- Pacientes e invitados maliciosos: Estos actores forman parte del ecosistema sanitario; pueden tener una intención maliciosa que, combinada con el acceso que tienen a los activos de la institución, puede causar un gran impacto.
- Atacantes remotos: En el caso de algunos hospitales, uno de los objetivos es la prestación de atención a distancia. Así que el uso de este equipo para acciones maliciosas podría ser un escenario posible cuando el atacante no está físicamente en el hospital.
- Otras causas: Las fallas ambientales o accidentales de equipos o software, o incluso el personal de mantenimiento externo, pueden causar incidentes de seguridad.

C. Análisis de vulnerabilidades.

Las vulnerabilidades prevalentes no sólo facilitan las acciones maliciosas, sino que también pueden aumentar la probabilidad y el impacto de los errores humanos y los fallos del sistema

1. Los dispositivos están dispersos por toda la institución de salud, esto significa que la seguridad física es prácticamente imposible para todos los componentes.
2. Específicamente para los dispositivos médicos, su vida útil es una desventaja muy importante que considerar. Los hospitales no cambian los escáneres de los equipos de Tomografía Axial Computarizada (TAC) o las máquinas de Resonancia Magnética Nuclear (RMN) cada 3 años y cuando compran los dispositivos puede que ya estén anticuados.
3. Los dispositivos de IO ejecutan sistemas operativos y aplicaciones embebidos con poca o ninguna capacidad de detección o prevención de malware.
4. El usuario real tiene poca o ninguna idea del funcionamiento interno de los dispositivos o de los flujos de datos precisos que producen. Con respecto a los dispositivos médicos, el personal clínico, el personal de TI y el paciente tienen poco o ningún conocimiento de este tipo.
5. A pesar de estar bien formados y ser conscientes de ello, los funcionarios pueden eludir medidas de seguridad tales como políticas y procedimientos si se perciben como innecesariamente inconvenientes.
6. Debido a las necesidades clínicas, es posible que se utilicen sistemas o dispositivos que no cumplan con los estándares de la organización o de la industria.

D. Ingeniería Social

La ingeniería social se refiere al método de influenciar y persuadir a las personas para que revelen información confidencial para realizar alguna acción maliciosa. Con la ayuda de trucos de ingeniería social, los atacantes pueden obtener información confidencial, detalles de autorización y acceder a detalles de personas engañándolas y manipulándolas.

Para comprender que es, como afecta y si se puede proteger la información de las organizaciones de ataques de Ingeniería Social requerimos conocer sus aspectos fundamentales, tipos de ataques, comportamiento y métodos de mitigación de vulnerabilidades entre otras cualidades.

1) Fases de un ataque

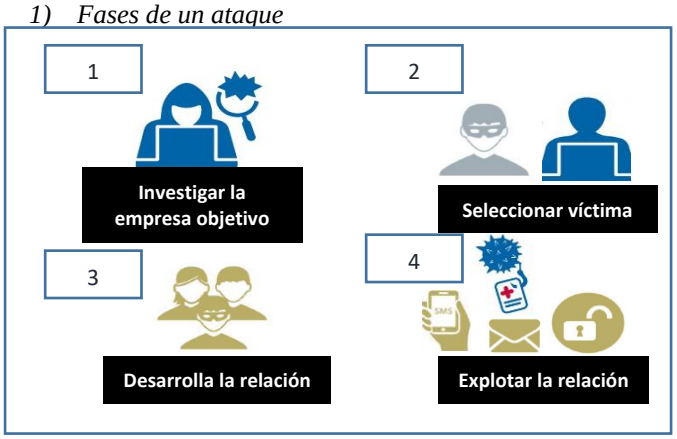

Fig. 1. Ataque de ingeniería social al personal de una Institución de Salud. Fuente. Propia

2) Tipos de Ingeniería Social

Existen 3 tipos de ataques de ingeniería social:

TABLA I. TIPOS DE INGENIERÍA SOCIAL

Tipo	
Basada en Humanos	• Posicionándose como un usuario final legítimo • Posicionándose como un usuario importante • Posicionándose como soporte técnico • Otras técnicas: – Eavesdropping, – Surfing on the shoulder, – Dumpster diving, – Tailgating, – Ingeniería Social inversa, – Piggybacking
Basada en Computadoras	• Ventanas emergentes, • Correo no deseado, • Instant Chat Messenger, • Hoax Letters, • Cartas en cadena, • Pop-ups, • Phishing, • Spear Phishing
Basada en Dispositivos Móviles	• Publicación de aplicaciones maliciosas • Reempaquetado de aplicaciones legítimas • Aplicaciones de seguridad falsas • Uso de SMS

Fuente: Autor

3) Previniendo amenazas internas

Se recomiendan técnicas de prevención para evitar la pérdida financiera y la amenaza a los sistemas de la organización por parte de personas internas o de la competencia. Se recomiendan los siguientes para superar las amenazas internas:

- Separación y rotación de deberes
- Mínimos privilegios
- Acceso controlado
- Registro y auditoría
- Políticas legales
- Archivar datos críticos

4) Contramedidas de Ingeniería Social

En primer lugar, para protegerse contra los ataques de ingeniería social, se debe implementar una serie de buenas políticas y procedimientos. El solo desarrollo de estas políticas no es suficiente. Para ser efectivo:

- La organización debe difundir las políticas a todos los usuarios de la red y proporcionar una educación y capacitación adecuadas. La capacitación especializada beneficia a los empleados en puestos de mayor riesgo frente a amenazas de ingeniería social.
- Después de recibir capacitación, los empleados deben firmar una declaración que reconozca que comprenden las políticas.
- Debe definir claramente las consecuencias por violar las políticas.

Las políticas y procedimientos de seguridad oficiales ayudan a los empleados o usuarios a tomar las decisiones de seguridad correctas. Dichas políticas incluyen lo siguiente:

- Políticas de contraseña
- Políticas de seguridad física
- Formación
- Directrices operacionales
- Privilegios de acceso
- Clasificación de la información
- Sistema de respuesta de incidencia apropiada
- Verificaciones de antecedentes de los empleados y proceso de finalización adecuado
- Autenticación de dos factores (TFA o 2FA)
- Defensas Antivirus / Antiphishing
- Gestión del cambio

E. Activos afectados

Entre los activos más afectados por los ataques de ingeniería social contra el personal de los hospitales se encuentran

- Dispositivos médicos en red
- Equipo de red
- Componentes de identificación
- Dispositivos cliente
- Sistemas de información clínica en red
- Sistemas de información de la empresa
- Centro de datos
- Información
- Personal
- Edificios

A través de la ingeniería social, un atacante puede tener acceso a los activos de las TIC de un hospital o institución de salud, incluidos los dispositivos médicos en red, los componentes de identificación, los dispositivos cliente, los sistemas de información clínica en red y los sistemas de información de la empresa. Con respecto a los activos no relacionados con las TIC, la información y el personal se ven afectados. La información puede ser fácilmente mal utilizada con el acceso a los activos de las TIC y la ingeniería social no sería posible sin el personal del hospital desempeñando su papel.

F. Criticidad

Alta - La criticidad es alta debido a la amplia gama de ataques de seguimiento que pueden ser posibles después de un ataque exitoso de ingeniería social. Los datos violados en el hospital, por ejemplo, incluyen información confidencial como el nombre del paciente, un número de registro médico, datos demográficos como direcciones y números de teléfono, fechas de servicio, montos de cargos por servicios recibidos en el hospital, el número de seguro social y los datos de nacimiento.

G. Probabilidad

Alta - La ingeniería social se ha convertido en un punto de inflexión para los ataques en el contexto de la atención sanitaria. Las personas son consideradas un eslabón particularmente débil en la cadena de seguridad de una organización. El personal del hospital a menudo carece de conciencia sobre la seguridad.

H. Efectos en cascada

La ingeniería social puede llevar al compromiso de la información sensible, como datos de los pacientes y registros de salud, así como la información financiera puede ser el objetivo. Debido al hecho de que los sistemas y dispositivos de información están intensamente conectados en los hospitales, un ataque exitoso de ingeniería social puede poner en peligro gran parte de la infraestructura.

I. Tiempo de recuperación y esfuerzos

Es difícil hacer una declaración general sobre el tiempo de recuperación y los esfuerzos después de un ataque de ingeniería social. El tiempo y los esfuerzos dependen mucho de las actividades de un atacante después de que un ataque de ingeniería social haya tenido éxito. Detectar y reaccionar rápidamente a un ataque es importante para mantener el tiempo de recuperación y los esfuerzos manejables. Sin embargo, no es improbable que los ataques sean persistentes y pasen desapercibidos durante mucho tiempo.

J. Buenas Prácticas

Entre las principales medidas que deben adoptarse en relación con los ataques de ingeniería social contra el personal de las instituciones de salud figuran las siguientes:

- Formación y sensibilización
- Políticas y procedimientos
- Organización de seguridad
- Auditorías

La forma más importante de protegerse contra la ingeniería social es la formación del personal con actualizaciones frecuentes. Es esencial que se tenga conciencia de los ataques de la ingeniería social en particular y de la seguridad de la información en general. Además, unas políticas claras en relación, por ejemplo, con la solicitud de verificación, el uso de los medios de comunicación social y la denuncia de personas o situaciones sospechosas pueden reducir el riesgo de ser víctimas de un ataque exitoso de ingeniería social. Además, es importante que haya funciones y responsabilidades claras para evitar y responder rápidamente a los ataques de la ingeniería social. Las pruebas de penetración de ingeniería social pueden ser una forma particularmente eficaz de crear conciencia de la amenaza.

K. Controles de un Sistema de Gestión de Seguridad de la Información.

Entre las buenas prácticas para minimizar ataques de IS es implementar los controles específicos para estos como ser:

TABLA II. CONTROLES PARA MINIMIZAR ATAQUES DE INGENIERÍA SOCIAL

Control	Sub control
Políticas de seguridad de la información	Orientación de administración para la seguridad de la información
Organización de la seguridad de la información	Organización interna
	Dispositivos móviles y teletrabajo
Seguridad en RRHH	Antes del empleo
	Durante el empleo
	Despido y cambio de empleo
Control de acceso	Requisitos del negocio
	Gestión de acceso de usuarios
	Responsabilidades del usuario
	Control de accesos a sistemas y aplicaciones
Seguridad física y del entorno	Áreas seguras
	Equipos
Seguridad en las comunicaciones	Administración de la seguridad de redes
	Transferencia de información

Fuente: Autor

L. Buenas prácticas organizativas

Las medidas organizativas incluyen, entre otras, el modelo de gobernanza de la seguridad, las políticas y procedimientos de seguridad, las normas y certificaciones, la formación y la sensibilización, la gestión de riesgos, las auditorías y evaluaciones y las cláusulas contractuales.

1. Gobernanza de la seguridad.

   C1 - Especifique las funciones y responsabilidades de seguridad

   C2 - Crear políticas y procedimientos de seguridad

   C3 - Desarrollar programas de capacitación y sensibilización

2. Gestión de riesgos

   C4 - Identificar riesgos, activos y amenazas

   C5 - Desarrollar un plan de contingencia

3. Cumplimiento y garantía

   C6 - Adoptar normas

   C7 - La preforma suele ser una auditoría de seguridad

   C8 - Realizar evaluaciones de seguridad

   C9 - Acordar cláusulas contractuales con los fabricantes

M. Buenas prácticas técnicas

Las medidas técnicas incluyen, entre otras, la gestión de activos y configuraciones, la monitorización de la red y la detección de intrusiones, la aplicación de parches y actualizaciones, la segmentación de la red y la gestión de autenticación y privilegios.

1. Ciberseguridad y medidas de protección (Arquitectura segura)
   - C10 - Implementar mecanismos de monitoreo y detección y prevención de intrusiones
   - C11 - Imponer la segmentación dinámica de la red y el uso de cortafuegos
   - C12 - Ejecute software antimalware
   - C13 - Realice copias de seguridad periódicas
2. Control de la seguridad de los activos
   - C14 - Configuración y gestión de activos
   - C15 - Aplique los procedimientos de parcheo y actualización
   - C16 - Hacer cumplir el control de acceso
3. Seguridad de los datos
   - C17 - Imponer el cifrado de datos
   - C18 - Clasificar datos
4. Móvil seguridad de componentes
   - C19 - Proteger los sistemas sanitarios remotos y móviles

IV. Discusión

La aplicación de las medidas de seguridad introducidas en la sección anterior y examinada en el contexto de los escenarios de ataques de ingeniería social, es necesaria, pero no suficiente, para garantizar un nivel adecuado de seguridad de la información en los hospitales e instituciones de salud a largo plazo.

La identificación de buenas prácticas sobre el tema de la ciberseguridad en las instituciones de salud, permite la identificación de cuestiones pendientes; en concreto, lo que aún queda por hacer para mejorar la ciberseguridad en el vasto ecosistema que los componentes de internet de las cosas (IO) introducen en la asistencia sanitaria. A continuación, se resumen las más importantes:

Brecha 1. Falta por traer sus propios controles de dispositivo.

Brecha 2. Necesidad de una herramienta automatizada de descubrimiento de inventario de activos.

Brecha 3. Falta de tecnología de listas blancas de aplicaciones (lista de software y versiones autorizadas).

Brecha 4. Necesidad de garantizar configuraciones seguras.

Brecha 5. Falta de programas de capacitación y sensibilización

Brecha 6. Administración remota de servidores, estaciones de trabajo, dispositivos de red, y otros, sobre canales seguros.

Brecha 7. Estandarización frente a la tecnología de TI.

Brecha 8. Desglose de la relación costo-beneficio.

V. Conclusión

Cualquier persona, organización, incluso los profesionales de la seguridad de la información, pueden ser víctimas de ataques de Ingeniería Social. Mientras exista una interfaz consciente entre los seres humanos, por un lado, y los sistemas y dispositivos, por otro, la Ingeniería Social persistirá, por lo que una buena concienciación a los empleados en todo nivel será muy necesario.

Referencias

[1] ESET, La seguridad como rehén Tendencias 2017. Bratislava: WeLiveSecurity, 2017.

[2] Knowbe4, Social Engineering. Recuperado de https://www.knowbe4.com/what-is-social-engineering, 2019.

[3] Verizon, Data Breach Investigations Report, 2019.

[4] ENISA, Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures, 2016.

[5] Ponemon Institute, Cost of Data Breach Study, 2019

[6] SGSI Blog especializado en sistemas de gestión de seguridad de la información. ISO27001 aplicado al sector salud. (2013). Recuperado de https://www.pmg-ssi.com/2013/11/iso-27001-aplicacion-en-el-sector-salud), 2013

[7] Sampieri, R. Metodología de la investigación, 2002.